12-1-2015

On Reliability of Smart Grid Neighborhood Area Networks

Shengjie Xu

Yi Qian

Rose Qingyang Hu

Received September 30, 2015, accepted October 25, 2015, date of publication November 19, 2015, date of current version December 1, 2015.

Digital Object Identifier 10.1109/ACCESS.2015.2502250

On Reliability of Smart Grid Neighborhood Area Networks

SHENGJIE XU[1], (Student Member, IEEE), YI QIAN[1], (Senior Member, IEEE), AND ROSE QINGYANG HU[2], (Senior Member, IEEE)
[1]Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, Omaha, NE 68182, USA
[2]Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84322, USA

Corresponding author: R. Q. Hu (rose.hu@usu.edu)

This work was supported by the National Science Foundation under Grant CNS-1423348 and Grant CNS-1423408.

ABSTRACT With the integration of the advanced computing and communication technologies, smart grid system is dedicated to enhance the efficiency and the reliability of future power systems greatly through renewable energy resources, as well as distributed communication intelligence and demand response. Along with advanced features of smart grid, the reliability of smart grid communication system emerges to be a critical issue, since millions of smart devices are interconnected through communication networks throughout critical power facilities, which has an immediate and direct impact on the reliability of the entire power infrastructure. In this paper, we present a comprehensive survey of reliability issues posted by the smart grid with a focus on communications in support of neighborhood area networks (NAN). Specifically, we focus on network architecture, reliability requirements and challenges of both communication networks and systems, secure countermeasures, and case studies in smart grid NAN. We aim to provide a deep understanding of reliability challenges and effective solutions toward reliability issues in smart grid NAN.

INDEX TERMS Smart grid, neighborhood area network, reliability.

I. INTRODUCTION

Smart grid is one of the most critical large-scale systems which adopt advanced communication technologies and modern control techniques to significantly improve the reliability and security of the power grid [1], [2]. It is featured by its two-way flows of electricity and information, based on which an optimized energy delivery network can be constructed [3], [4].

In smart grid communication networks, neighborhood area network (NAN) offers power distribution with the ability of monitoring and controlling electricity delivery to each household, thus NAN fulfills the communication gap between smart grid wide area network (WAN) and home area network (HAN) [5]. In the network architecture of NAN with advanced metering infrastructure (AMI), as shown in Fig. 1, massive metering data is firstly aggregated from thousands of smart meters located at different homes each with a HAN. Energy usage data along with metering data are reported to a local concentrator, which acts as the master gateway of a NAN, through multiple data aggregation points (DAPs). Without doubt NAN lies in one of the most crucial segments in communication infrastructure of smart grid.

However, considering the features of smart grid, reliability is one of the basic but the most important requirements for designing such a highly advanced system in smart grid. A heavy dependence on information networking inevitably yields the smart grid to potential reliability issues associated with both communications and networking systems. This fact truly increases the risk of compromising a reliable and secure power system. For example, it has been shown [6], [7] that possible malfunction and network failure may lead to a cascading impact across communication components and a variety of severe consequences in grid systems, from customer information leakage to a cascade of failures, such as massive blackout and destruction of infrastructures.

The term reliability means the probability that a system performs a specified service throughout a specified interval of time [8]. In communication networks for smart grid, potential vulnerability of system failures is still in a high rate, while there exists a risk of malicious cyber attacks to communication systems. According to the recommended communication quality of service (QoS) and availability requirements from U.S. Department of Energy (DoE), the reliability for smart grid AMI networks is set between the range

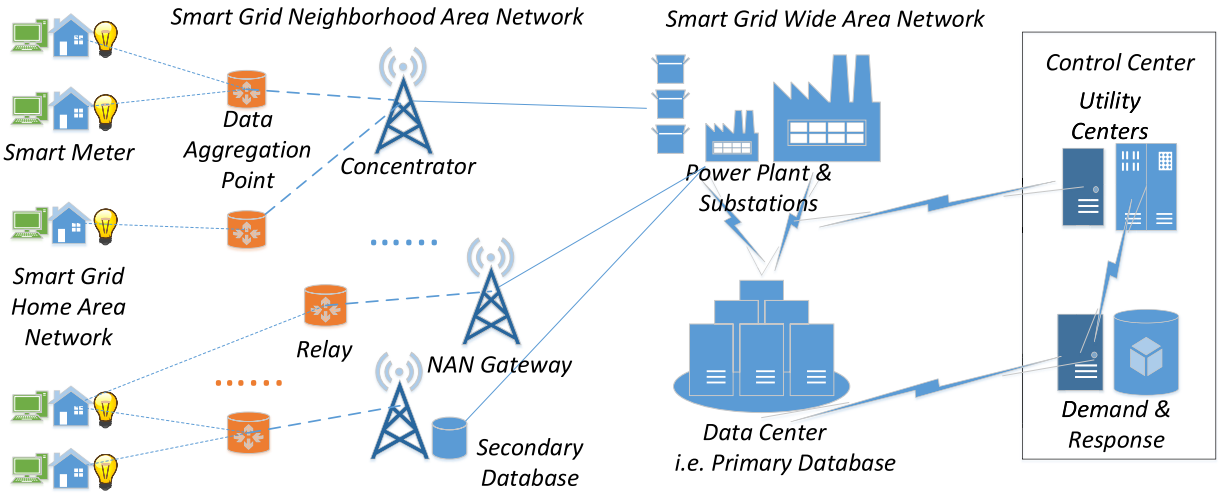


FIGURE 1. A communication architecture for the deployment of smart grid and its utility networks.

of 0.99 - 0.9999 [9]. Therefore, reliability of NAN plays a critical role in providing assured services in smart grid communication infrastructures [10], [11], and remaining a high reliability in smart grid NAN guarantees the availability of continuous data communication services [12].

As a result, we are motivated to investigate reliability issues in the smart grid NAN, which is of critical importance to the neighborhood area network design and has been considered as one of the priorities for smart grid communications [13]–[15]. In this paper, we discuss the reliability requirements posed by the smart grid NAN and their impact on communication network design. We provide an overview, analyze potential reliability challenges, review existing solutions, and present case studies for communication reliability in smart grid NAN. More specifically, the following topics are discussed in the paper:

- Smart grid communication architecture: We first describe the fundamental architecture of communication networks in smart grid, with a focus on NAN and AMI, followed by communication standards for NAN.
- Communication and system reliability of NAN: We focus reliability issues which mainly come from communication networks and systems, we review those reliability challenges, and provide basics for reliability analysis.
- Countermeasures and recovery: To efficiently counter-react reliability issues, it is essential to widely deploy prevention, detection, mitigation, and recovery strategies throughout NAN. Therefore, we present some discussions on existing solutions, including network design and system defense countermeasures, by considering applications in smart grid NAN.
- Reliability case studies: Several reliability issues in NAN are investigated and we provide a comprehensive analysis for NAN in smart grid, using fault tree analysis on potential system failures and attack countermeasure tree to identify specific detection and mitigation strategies on malicious cyber attacks to communication systems in NAN. We also conduct a simulation study that the self-healing ability of NAN is enhanced through proper topology design. The simulation study evaluates both reliability and networking efficiency of the communication networks in NAN.

The rest of this paper is organized as follows. In Section II, we introduce a fundamental architecture of communication networks in smart grid. In Section III, we present basic concepts for reliability analysis. In Section IV, we present the communication reliability issues and challenges for nodes and links. In Section V, we present the reliability issues and challenges from the NAN systems level. In Section VI, we discuss the countermeasure strategies for NAN reliability. We present case studies and discussions in Section VII. We conclude the paper in section VIII.

II. COMMUNICATION ARCHITECTURE

In this section, we present a communication architecture in smart grid networks, with a focus on NAN and AMI, followed by communication standards for NAN.

A. WAN, NAN AND HAN

According to NIST's conceptual domain model [16], smart grid power systems consist of seven domains, including power generation, transmission, distribution, power operation, service provider, markets and customer, which are normally deployed over a large geographical area. The smart grid communication infrastructure is based on a comprehensive design with heterogeneous communication technologies. The communication structure between back-haul aggregation points to the core backbone utility center is carried over different types of communication networks, such as star, mesh networks and fiber, wireless networks.

From the perspective of energy transmission, we present a hierarchical smart grid network structure including three domains, i.e. a wide area network (WAN)

domain connecting power generation, transmission and distribution systems, a community based neighborhood area network (NAN) domain, and a smart appliance based homework area network (HAN) domain. A brief description of the three categories is shown below.

- **Wide area network** provides the communications among electric utility and substations. Basically, the WAN consists of bulk electrical power generation plants, a large number of distributed substations and transformer equipments, which require real-time measuring and monitoring to achieve wide area situation awareness. Hence, the WAN requires to maintain a reliable high-bandwidth backbone communication network that handles long-distance data transmission with advanced sensing and monitoring applications. In summary, the wide area network connects the power grid control centers and the data concentrator of each NAN, and transmits energy data in a high-speed manner [17], [18].
- **Neighborhood area network** is described as the bridge network between customer sides and substations, where intelligent electronic devices (IEDs) are widely deployed to control and collect data from nearby data points. NAN incorporates advanced two-way communication technologies between NAN concentrators and smart meters, delivers the information of power usage and system control with different types of requirements. In a NAN, the data transmission rate is not as high as in WAN, while the transmission power is relatively low for the short range transmission, compared to the one in a WAN. One of the unique characteristics of smart grid NAN is that wireless communication technologies, especially low bandwidth channels, are widely adopted in NANs. Those channels are highly robust for reliable data communications, which meets the utility requirements for reliability and resilience. NAN is also extensively deployed by advanced metering infrastructure (AMI) and it is rapidly expanding the range of its application areas, e.g., advanced distribution automation and integration of distributed energy resources [19].
- **Home area network** is mainly categorized in the customer domain, with many types of intelligent electric appliances and smart meters, most of which are usually installed in buildings and home areas. Home area networks support low-bandwidth communications between home electrical appliances and smart meters. Bandwidth needs are between 10 and 100 Kbps per device and there is no urgent need for low latency [9].

B. ADVANCED METERING INFRASTRUCTURE

As illustrated in Fig. 2, AMI creates a two-way communication network between smart meters and utility systems, as well as the integration of advanced sensors, monitoring nodes, and data management systems. AMI enables the collection and distribution of metering data information [20]–[23]. One of the core components, meter

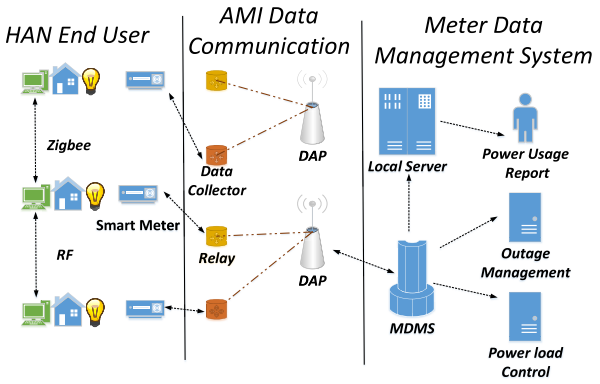


FIGURE 2. A communication architecture of AMI.

data management system, handles the huge amount of data and manages the raw data to create meaningful information and messages for customers, assisting them in using energy intelligently.

The selection on communication technology for AMI mainly depends on the coverage and the number of customers in a certain area, the availability of the Internet connection, the expected energy efficiency, scalability, the required data rate, and the expected communication delay. Fig. 2 shows an example on communication architecture from residential areas to data collector units and from data collector units to meter data management systems in AMI.

C. COMMUNICATION STANDARDS FOR NAN

Several wireless standards, such as IEEE 802.11, IEEE 802.15 and IEEE 802.16 are recommended to be adopted in smart grid NANs [24]. Among all the IEEE standards, two IEEE communication standards are more favorable in NAN, IEEE 802.11s and IEEE 802.15.4g. 802.11s is an amendment for mesh networking and it addresses some issues on networking of smart grid NANs. 802.15.4g specifies physical layer (PHY) and MAC layer architecture of smart grid communication networks.

1) IEEE 802.11s

IEEE 802.11s is a standard which is recommended for smart grid NANs [25], [26]. Initially, IEEE 802.11s was derived from the family of IEEE 802.11 standard, the goal of which is to create an amendment to extend IEEE 802.11 MAC protocol for wireless mesh networks (WMNs). One of the most important features of IEEE 802.11s is to support frame delivery and route selection at media access control (MAC) layer through radio aware metrics [17]. Aside from the revision towards the MAC protocol, the PHY layer of IEEE 802.11s remains the same as the IEEE 802.11, thus the data transmission will be in a high-speed mode. This guarantees a reliable protocol for high-speed wireless applications in a smart grid NAN.

In the topology of an IEEE 802.11s mesh network, a central gateway is designated and deployed for data transmission to mesh stations. In this meshed network, access points offer the

access to end users with either a static or dynamic state, and aggregated information could also be transmitted to gateways through multi-hop paths. In this standard, a self-configured multi-hop wireless network could be formed among wireless devices. For routing scheme, the hybrid wireless mesh protocol (HWMP) is the default routing protocol for IEEE 802.11s [27].

2) IEEE 802.15.4g

The standard IEEE 802.15.4g [28] was developed by the IEEE 802.15 Task Groups in 2012, with an achievement of presenting a PHY amendment and MAC modifications. Its goal is to specify the requirements of outdoor low data rate and wireless smart metering utility network (SUN), and facilitates large scale process control applications in a utility network. The devices in SUN can operate in an environment with large-scale and low-power wireless applications [29]. Usually, a SUN contains a large group of outdoor devices to cover wide areas geographically. Therefore, peer-to-peer multi-hop techniques are usually adopted to form the communication links between end devices and access points [17].

In summary, IEEE 802.15.4g is a wireless networking standard enabling inter-operable communications between certain smart grid devices, including smart meters and smart home appliances. We can observe that IEEE 802.15.4g is used mainly for NAN connectivity, while IEEE 802.16 can be used for WAN connectivity and can relay signals from IEEE 802.15.4g back to utility backbone.

III. RELIABILITY ANALYSIS

For information communication technology (ICT) systems, reliability study is always important. Reliability is characterized as the ability to execute a defined function under specified conditions for a known period of time [30]. By its definition, the term ''reliability'' refers to the ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time. In the content of this paper, the ''item'' could be a component, a subsystem, or a system.

A. RELIABILITY FUNCTION AND FAILURE RATE

The reliability function $R(t)$ refers to the probability that the unit does not fail in the time interval $(0, t]$ or the probability that the unit survives the time interval $(0, t]$. If we denote $F(t)$ as the probability that the unit fails within the time interval $(0, t]$, then

$$F(t) = P(T \leq t) = \int_0^t f(u)du, \quad \text{for } t > 0, \tag{1}$$

where a failure density function $f(t) = \frac{d}{dt}F(t)$. In this case, our reliability function $R(t)$

$$R(t) = 1 - F(t) = P(T > t), \quad \text{for } t > 0. \tag{2}$$

is presented in this form. Let $P(t < T \leq t + \Delta t | T > t)$ denote the probability that a unit will fail in the time interval $(t, t + \Delta t]$, given that the unit is functioning at time t, we can present the variable of failure rate $\lambda(t)$ as

$$\begin{aligned}\lambda(t) &= \lim_{\Delta t \to 0} \frac{P(t < T \leq t + \Delta t | T > t)}{\Delta t} \\ &= \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} \frac{1}{R(t)} \\ &= \frac{f(t)}{R(t)}.\end{aligned} \tag{3}$$

Since we know $f(t) = \frac{d}{dt}F(t) = -\frac{d}{dt}R(t)$ and $\lambda(t) = \frac{f(t)}{R(t)} = -\frac{d}{dt}\ln R(t)$, we can derive from above that the reliability function $R(t)$ is denoted as

$$R(t) = \exp(-\int_0^t \lambda(u)du). \tag{4}$$

B. BASIC METRICS FOR RELIABILITY STUDY

Since we already know the relationship between reliability function and failing rate, our next goal is to find out how reliability is closely related to the expected time between failures. In this paper, reliability study always specifies a mission time duration t. We present the first metric for reliability study, called Mean Time To Failure (MTTF), which could also be regarded as the mean functioning time of the item under study. In an ideal case,

$$MTTF = \int_0^\infty tf(t)dt = \int_0^\infty t[-\frac{d}{dt}R(t)]dt. \tag{5}$$

We then present the second metric, called Mean Time to Repair (MTTR), which is the average time to restore full functionality to an item. This metric varies since it may depend on the time to travel to this item, to diagnose, to remove, even to isolate and to replace the corresponding parts. It is obvious that the third metric Mean Time Between Failures (MTBF) has a certain relationship with them. If the availability A of an item means the ability to perform the stated function over time t, we have the following relationship of A:

$$A = \frac{MTTF}{MTTF + MTTR} = 1 - \frac{MTTR}{MTBF}. \tag{6}$$

The relationship between the reliability metrics are shown in Fig. 3. More reliability analysis will be discussed in the rest of this paper.

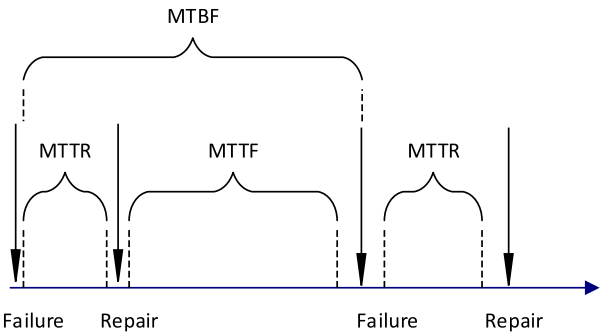


FIGURE 3. Relationship between basic reliability metrics.

IV. COMMUNICATION RELIABILITY FOR NODES AND LINKS

Communication network reliability is a basic requirement for smart grid NAN, which defines the availability of data transmission links and nodes. Smart grid NAN should have a self-healing mechanism through proper topology and routing design, so that abnormal operation of a single node or a few nodes will not affect the performance of the entire network. Besides that, common performance metrics can also be a huge factor impacting reliability of communication networks.

In this section, we mainly discuss communication nodes and links towards network failure, as well as the proper networking design to improve network reliability. As we discussed earlier, a NAN provides two-way communications between smart meters and a master gateway, i.e. a data concentrator, through multiple DAPs. In this network, the entire communication topology is comprised of thousands of nodes, and it is interconnected by various wireline and wireless links using different communication standards. A single node failure or a single link failure would degrade a small range of communication network, thus lower the reliability to part of a NAN. In dealing with a networking failure for any communication nodes or links, a NAN should have a self-healing capability through proper topology and networking design.

A. RELIABLE NETWORKING DESIGN IN NAN

In smart grid NAN, a mesh network is a flexible network with the characteristics of self-healing, self-configuration and high scalability services [31]. Wireless mesh network in smart grid NAN consists of a group of nodes, where new nodes can join the group and each individual node can act as an independent router. The self-healing advantage of the network enables the communication signals to find an alternative route through active nodes, if any node is forced to drop out of the topology [32]. For smart grid communication network in North America, RF mesh-based system are very popular [33].

In practice, a good coverage of mesh networking can provide an enhanced capability of multi-hop routing in urban and suburban areas. Some companies use mesh networking for smart grid applications due to the redundancy and high availability features of mesh technology [34]. A multiple-gateway mesh network topology for smart grid NANs was presented in [25]. The authors stated that a mesh network is required for NANs to meet reliability, self-configuration, and self-healing requirements of smart grid applications. In a large-scale NAN, multiple data aggregation points (DAPs) are needed to reduce network congestion and improve reliability. In this architecture, with IEEE 802.11s, each DAP forms a tree-based sub-network and a DAP is the root node. The authors emphasized the features of this network such that each meter has a separate path to reach gateway and such a topology can enhance self-healing and self-organization of the network in emergency situations. However, to acquire this feature, packet scheduling algorithms must be used to support optimal gateway selection.

B. NODE & LINK FAILURE

In node failure, each wireless mesh network consists of a set of DAPs and they gather data from a group of nearby smart meters. If the status of a DAP has changed to a failure mode, or lost its network connection to the rest of the nodes, this failure event should be notified to all other active neighbors. One study [35] suggests that a possible NAN topology would be a complete fully meshed graph, which makes the graph structure much more resilient in terms of communication reliability. This scheme is practically reliable for communication node failures in the neighborhood networking design, however, the communication overhead such as routing broadcast and discovery would be increased in an exponential way.

In link failure, the wireless link is not as easy to be failed as the wireline link since the majority communications of a NAN are based on wireless technology. A wireless link failure can not occur normally unless either a source or a destination node fails or is attacked by a malicious adversary. Moreover, the communication media for wireless equipment to transmit is based on open air, thus it is not as easy to be cut out on a physical object as a wireline equipment is. However, both wireline and wireless communication links suffer from passive attacks, which will be discussed in the section later in this paper.

C. GRAPH ANALYSIS

Graph theory analysis is often studied as a first step in reliability analysis. By using graph analysis, we can model a NAN as an interconnected graph, rank the priority of each node and link, and determine the critical components to model and protect in detail. Through graph theory analysis, we can identify which nodes and links are crucial for incident response and need for greatest protection, and specify the node failure and its corresponding effects in a simulation model. An undirected graph $G = (V, E)$ is a mathematical structure consisting of two sets V and E, where $V = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes and $E = \{e_1, e_2, \ldots, e_l\}$ is the set of edges. Considered a NAN, represented by the undirected graph $G = (V, E)$, elements of V can be represented as smart meters, DAPs and data concentrator, and elements of E can be represented as wired and wireless communication links.

For graph structures of a NAN, the potential options of graph types are tree, star, chain, ring and mesh graphs. However, in order to achieve overall reliability of communications in NAN, tree, star and chain graphs are not preferred since tree graph is usually considered as a cheap design with poor reliability, star graph has only one center node with a degree larger than 1, and chain graph is basically an alternative form of tree graph with no node carrying a degree larger than 2. Ring graph is more reliable with each mode having a degree of 2 and 1 additional link compared to tree graph, but it is still not a practical solution. For graph structure in a smart grid NAN, mesh graph based networks are widely adopted. In a mesh network, each node has a degree of 2 or more and it can form a connected graph in which every pair

of distinct nodes has a path between them. Based on the graph metric Beta Index $\beta = l/n$ [36], which represents the level of connectivity in a graph and the robustness of a graph structure, we can find out that the Beta Index of a tree graph is $\beta < 1$, a ring graph is $\beta = 1$, a mesh graph is $\beta > 1$. A fully mesh graph is resilient with $\beta = (n-1)/2$, however from a trade-off perspective, the cost is that there are $n(n-1)/2$ links to connect n nodes.

For evaluating the robustness and connectivity of network structure in a NAN, metric like clustering coefficient $cc_G(v_i)$ of a node v_i in graph G measures how connected a graph is locally. Given the degree d_{v_i} of a node v_i,

$$cc_G(v_i) = \frac{2y}{d_{v_i}(d_{v_i}-1)}. \tag{7}$$

where y is the number of links between neighbors of v_i. With smaller value of $cc_G(v_i)$, we can mark the communication node v_i being less dependent and reliable from other communication nodes in a specific location in NAN.

Additionally, it is crucial to identify the critical nodes in NAN, since the attacks and failures on these nodes would bring the biggest impact. Although there are no fixed ways to define critical nodes, common approaches can be adopted as follows.

- Identify the nodes with maximum degree
- Identify the nodes with most networking traffic
- Identify the node and link whose failure will separate the graph
- Identify the nodes with greatest number of shortest path
- Identify the nodes with smallest clustering coefficient

D. SMALL-WORLD NETWORKS

Small-world networks refer to a class of graphs in which nodes are highly clustered such that most nodes are reachable from each other by only a small number of hops [10], [37]. In communication network reliability study, work can be explored when the NAN location graph is also a small network. The goal is to reach most of the nodes using a small number of hops.

To identify a network being a small-world network, the general steps are presented as follows. Finding out the degree of each node will be the first step. Count the number of nodes with degree of 1, 2, 3, etc, and divide these counts k by the number of nodes in the entire network. This gives us the frequency of nodes with a certain number of links. Based on the node frequency, a histogram can be plotted starting with the frequency of nodes with 1 link, then 2 links, 3 links, etc. The resulting histogram has a certain shape, i.e., the frequency counts will decline as the number of links increase. If the rate of decline approximates the curve $(1/k)^p$, where p is greater than one, then the network is a small-world network.

Theoretically speaking, for a NAN location graph with a small-world behavior, it is possible that packets are delivered to their destinations through only a small number of nodes. From this perspective, the idea of small-world network could be applied to network design and to improve the reliability of a certain NAN with highest priority.

V. COMMUNICATION SYSTEM RELIABILITY FOR NAN

Communication system reliability of a NAN in smart grid plays a crucial role in improving end-to-end AMI communications. From the system perspective, an unreliable communication system that periodically malfunctions and fails would degrade the reliability of a power management system significantly. Communication networks that delay or drop messages could degrade the system reliability of a control center.

Besides the system malfunction aspects, power outage incidents are crises that most electric utilities have faced as well. When it comes to uncertainty level, network vulnerability, various cyber attacks and unpredictable natural disasters are also the major factors that gain a crucial impact on AMI for providing unreliable services in a NAN.

For the architecture of NAN, four types of components would mainly be affected by the following reliability issues from the system level. A home gateway, i.e., a smart meter, collects household data and transmits them to a local DAP, which is also capable of relaying data from other meters. A DAP station represents a neighborhood gateway node. A relay station relays data from remote DAPs. A master gateway, i.e., the data concentrator, is the master access point of utility backbone. For a NAN in smart grid, main reliability issues occur within these four categories, namely, a) system malfunction; b) power outage; c) cyber attacks; d) natural disasters.

A. SYSTEM MALFUNCTION

By its definition, system malfunction is one type of failures for computing systems. For a smart grid NAN, most of the system failures are either in a small range or inside a single component, and relatively they would not affect the entire communication networks in a large scale. However a simple system malfunction could trigger a series of chain reactions to bring avalanche cascading failures (e.g. power outage) in smart grid due to the lack of the effective real-time management.

In order to improve reliability in NAN, efficient risk detection and mitigation schemes are necessary to reduce the potential risks brought by system malfunctions. For a simple system, it should be deployed with a powerful detection scheme as a redundancy to enhance its reliability. For a considerably complex system, it is normally equipped with multiple modules, e.g. CPU module M_1, database module M_2, sensor module $M_3, \cdots$, etc, to sustain its functionality. We use λ and μ as the notations for the system malfunction rate and the repair rate respectively. In this case, $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3$ denote the failure rates and repair rates of module M_1, M_2 and M_3 in a complex system respectively. If one of the module is in malfunction, the immediate detection scheme would be effective automatically and the corresponding repair scheme is then activated for troubleshooting correspondingly.

As we discussed earlier, reliability metrics can be used to indicate the reliability degree of system malfunction and analyze the most available improvement for system reliability [9]. In this study, reliability metrics mainly include mean time between failures (MTBF) and mean time to repair (MTTR). MTBF and MTTR can be expressed as

$$MTBF = \frac{1}{N}\sum_{i=1}^{N}\lambda_i, \tag{8}$$

and

$$MTTR = \frac{1}{N}\sum_{i=1}^{N}\mu_i. \tag{9}$$

respectively.

The availability (A) and unavailability (UA) can be described as

$$A = \frac{MTBF}{MTBF + MTTR}, \tag{10}$$

and

$$UA = \frac{MTTR}{MTBF + MTTR}. \tag{11}$$

respectively.

B. POWER OUTAGE

Power outage is defined as the loss of the electricity supply in a certain period. Any failure of short circuits that failed at power stations, and physical demages in any transmission or distribution lines can be reasoned for major power outage events. Most electric utilities have the experience of power outage crisis. The Northeast blackout in 2003 was a widespread power outage resulting in a $10 billion loss [38], based on a report by ICF consulting. Hence, outage detection, management and restoration are very critical for the continuity of reliable electricity delivery, QoS and customer satisfaction.

Recent discussions and activities aim at improving outage management processes by using smart grid technologies, specifically the ones adopted in neighborhood area network. In one case, AMI data integration into outage management system (OMS) can achieve advanced customer services, improve OMS reliability, outage notification and restoration notification [19]. There are several ways in the integration of AMI and OMS to improve the performance of OMS, and the advantages brought by the integration are promising. For example, an outage management process is usually initiated by an outage report from a customer call. In the AMI and OMS integration case, the outage notification message from AMI meters will be sent to the OMS very fast even if it is not reported by the customer, such as during the moments when customers are unavailable. In summary, the integration between AMI and OMS will not only improve the accuracy of reliability reports, but also reduce the manpower needed to collect and analyze outages for the reports.

However, to achieve such an integration and improve the reliability of OMS, we still need to address the requirements and the challenges.

- *Requirements:* Communication requirements will affect all three phases of outage management, detection and recovery. The main purpose of outage management is to respond to power outage more quickly, hence to achieve a latency of 2000ms and 56kbps bandwidth required by any OMS [9], [19].
- *Challenges:* OMS still needs to be integrated with other systems and requires a good quality of data. Furthermore, integration of advanced wireline and wireless communication networks, high-performance computers and specialized software applications are essential for an advanced OMS.

C. CYBER ATTACKS

Cyber attacks remain as one of the biggest issues to system reliability. In this section, we will focus on the impacts of system reliability brought by cyber attacks. In smart grid NAN, cyber attacks could be mainly categorized as active attacks and passive attacks [39].

For active attacks, the primary security objective for a NAN in smart grid should focus on the detection of potential attack events, mitigation of any current attack events and recovery of post-attack events. For possible active attacks, it is evident that a distributed denial of service (DDoS) attack is one of the most dangerous security threats to all components in NANs. Meanwhile, a secure networking design for routing protocol is critical for enhancing the resilience and reliability to system components in NAN. In an open network, potential routing attacks could be easily conducted by injecting a false link-state advertisement (LSA) to open shortest path first (OSPF) routing protocol, which is one of the widely used intra autonomous system (AS) routing protocol. When such incidents occur, massive metering data transmissions would be jeopardized in a large scale, and the MTTR of smart grid communication systems to such events takes relatively longer than any other failures. Therefore, it is urgent to build a complex mechanism for detection, defending against, and recovery from any cyber attack.

On the other hand, passive attacks to a NAN in smart grid are not as recognizable as the active ones. Eavesdropping, monitoring and traffic analysis are very difficult to detect since those events do not involve any alteration of data. Therefore during the data transmission, neither the sender nor the receiver is aware of any malicious event such as the content of data messages being read by an adversary. Although most of the passive attacks could be prevented by deploying strong modern cryptosystems, the computation overhead for such data encryption and decryption is relatively high as well.

D. NATURAL DISASTERS

A natural disaster is a major event from natural earth incidents to any critical communication systems. Such disasters would cause severe life loss or economical loss and damage valuable

properties within a vulnerable area [40], [41]. In smart grid communication infrastructures, NANs play an important role in supporting power utilities and customer communities, and also fight against natural disasters to reduce their impacts. Several studies [42] have focused on the impact of natural disasters that bring power outages and failures on AMI communication systems. Since smart grid NAN lies at the edge part of the power distribution domain, it is worth investigating the cause and the effects on a affected NAN by natural disaster.

In the rest of this paper, we mainly consider the impact of disasters on the affected NAN and quantify the level of reliability of communication services during network failures, explore some effective methods to mitigate the potential vulnerability on network infrastructures, and propose an effective solution for recovery from severe disasters.

VI. COUNTERMEASURES TO RISKS

When an incident occurs in a NAN, fast and accurate reliability analysis should be assessed as soon as possible. Once this assessment is done, efficient and effective countermeasures need to be chosen and the system would start to develop a protection strategy to prevent the incident going on. In order to achieve reliability levels that satisfy the industrial requirements, a NAN in smart grid should be performed in a balanced way so that they will function normally and prevent potential threats efficiently.

With that point in mind, we present the countermeasure strategies and risk analysis for reliability issues as follows:

A. PREVENTION

Prevention strategy is the very first effective approach which attempts to minimize the risk of accidental or intentional intrusions. In this strategy, the main goal is to avoid the risk, by moving secure systems to hazard-free zone. Possible approaches to be deployed in NAN include performing encryption and authentication schemes to pursue confidentiality and integrity, deploying interruption prevention, and facilitating risk analysis process to secure the networking environment.

B. DETECTION

Detection strategy is the techniques and programs used to ensure early detection, interception and response of security breaches. The status of detection applications should always be set as monitoring to detect any threat if it occurs. Intrusion detection and remote intrusion monitoring are normally deployed in NAN. Intrusion detection systems (IDS) can work efficiently, however it requires a large amount of history data for pattern recognition.

C. MITIGATION

The main idea of mitigation is to adopt techniques to reduce the impact of risk by implementing countermeasures and control schemes. The goal is to mitigate risks to a minimum extent. Mitigation schemes could be provided from the perspective of physical protection, cyber security techniques and network redundancy. One example on network access control is to separate accidental incidents from deliberate incidents.

D. RECOVERY

Recovery strategy is a planning and response service to rapidly restore a secure environment and investigate the source of the breaches. The goal is to provide means to recover if threat occurs. An alternative approach is to transfer the risk to other parties. This may require security level agreements among utility parties.

VII. CASE STUDIES

A. BACKGROUND

In this case study, we investigate two aspects of smart grid NAN. One is the reliability of communication system when it comes to system failure, the other is the risk analysis to a malicious cyber attack targeting a routing scheme in NAN.

The first step towards reliability study involves designing a model that helps quantify reliability in terms of key attributes such as the loss caused by failures and attacks, or the gain obtained by a reliable countermeasure [43]. Quantitative reliability analysis provides precise measurement of system risks based on modeling and analysis together with historical data, and it could assign numerical values to components and calculate potential loss [8]. The goal of performing such a quantitative risk analysis is to examine the potential vulnerabilities and threats to a NAN, and to mitigate risks in a minimum extent.

B. FAULT TREE ANALYSIS ON SYSTEM FAILURES

Fault tree analysis is a top-down system failure analysis, which incorporates probabilistic reliability examinations to construct and analyze fault tree diagrams to system components using Boolean logic [44]. In this study, we adopt fault tree analysis to exam the data collection module to NAN in smart grid.

In a NAN, massive metering data is generated from thousands of local smart meters and then transferred through multiple DAPs and finally aggregated by a concentrator. The concentrator acts as the master gateway of a NAN, containing a secondary database for temporary data storage and message integrity check. The effects of incorporating fault tree analysis are demonstrated via the module of data collection, which is shown in Fig. 4. For a complete data collection module, its

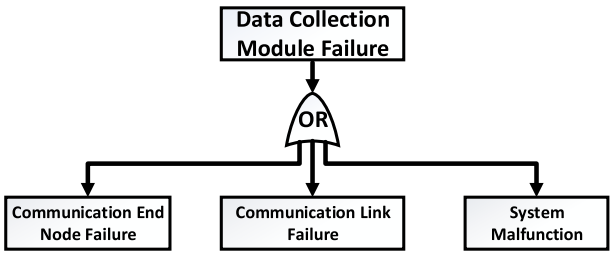


FIGURE 4. System failure model of data collection module.

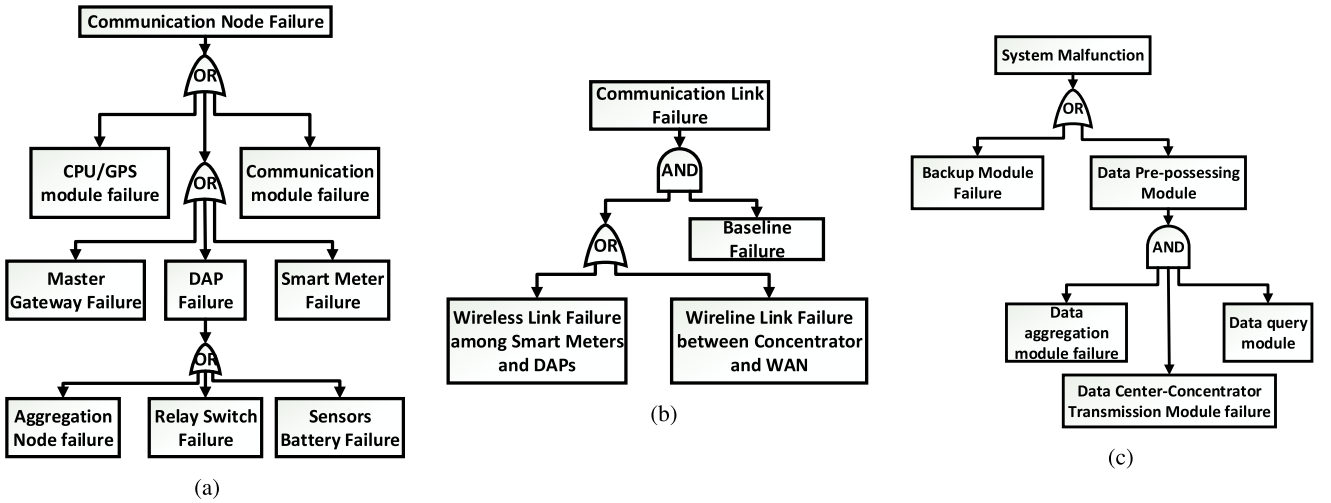


FIGURE 5. Fault tree analysis on each failure. (a) Communication node failure. (b) Communication link failure. (c) System malfunction.

failure could be resulted from communication node, link or system malfunction. In Fig. 4, each sub-incident is connected through an *OR* gate to combine all the possibilities.

Potential failures on communication nodes, links and system malfunction will impact the reliability of this module dramatically and may bring a cascading failure to the entire network, as reflected in the fault tree model. In Fig. 5, each top node indicates the source event that causes the failure. Each descendant represents a single fault event, and the combination of them results the likelihood of the occurrence on a parental event. In this case, *AND* and *OR* gates are both the symbols describing the relationship between input and output events. The fault tree analysis of failures to communication nodes, links and system malfunction is shown in Fig. 5a, Fig. 5b, and Fig. 5c, respectively.

In NAN, most common communication node failures occur in three components: data concentrator, data aggregation point and smart meters. As shown in Fig. 5a, DAP failure mostly occurs from failures of relay points, aggregation node and sensor batteries. In Fig. 5b, communication link failures are commonly affected based on the topology design and the stability of communication technologies. In Fig. 5c, system malfunction could happen at many more sectors, from one single component to an integrated system.

Fault tree analysis provides a detailed view of probabilistic risk analysis of a system in terms of infrastructure reliability. Not only does this approach present a straightforward view of both the availability and unavailability of selected components in a system module, but also it indicates the time interval of a component failures during one year and the corresponding repairing time period in hours. However, fault tree analysis does not incorporate any recovery or defense mechanism, which is a huge drawback to today's approaches in reliability study. Therefore there exists a certain limitation in adopting this method in terms of defending and mitigating the system risks.

C. ATTACK COUNTERMEASURE TREE ON CYBER ATTACKS

Based on the security model of attack tree (AT), attack countermeasure tree (ACT) security model is developed to take into account attack events as well as countermeasure events, which are demonstrated in the form of detection and mitigation mechanism. ACT is a modified attack tree to include mitigation and detection of attacks, and it quantifies security in terms of attributes such as the loss compromised by attacks or the gain obtained from a security countermeasure [45]. In an ACT, there are three distinct events: attack, detection and mitigation. For communications in a smart grid NAN, there exist many types of cyber security attacks jeopardizing the working order of an AMI. One typical example of such malicious attacks is the attack targeting at OSPF routing protocol, by injecting false LSA packets. In this study, we adopt the method of ACT for a quantitative analysis. We show an ACT example for false LSA attack in Fig. 6.

In this ACT, the legend indicates the category of events. The top event is associated with the set of all mincuts. In order to seek a feasible solution for reliability study, mincuts of an ACT represent attack and countermeasure scenarios. Considering attack scenarios such as sending malicious commands or altering configuration of a compromised router, the corresponding countermeasures would include 'traceroute' as one of the most popular detection mechanisms for spoofed routing messages, and sequence number randomized as the corresponding mitigation technique. The top event in an ACT can be represented as a boolean function $\overline{\Phi(X)}$ of each leaf node event. $\overline{\Phi(X)}$ represents the complementary boolean function for the ACT in Fig. 6, where X is a state vector for ACT and x_{A_i} is a boolean variable such that $x_{A_i} = 1$ when event A_i is active and $x_{A_i} = 0$ when event A_i is mute.

Based on this ACT, we can identify that the mincuts are $\{(A_2), (A_{12}, A_{111}), (A_{12}, A_{1121}), (A_{12}, A_{1122}), (A_{12}, A_{1123})\}$.

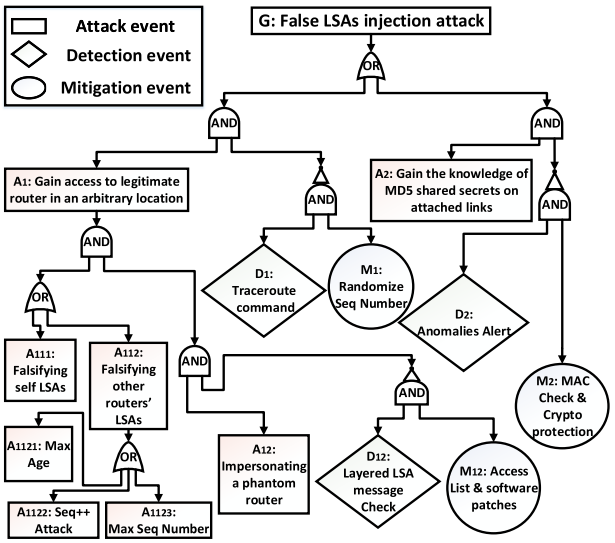


FIGURE 6. An ACT example for injecting a false LSA.

The boolean function for this can be expressed as

$$\overline{\Phi(X)} = x_{A_{111}}x_{A_{12}} + x_{A_{1121}}x_{A_{12}} + x_{A_{1122}}x_{A_{12}} + x_{A_{1123}}x_{A_{12}} + x_{A_2}. \quad (12)$$

The attack countermeasure scenarios, i.e., the mincuts, of the ACT in Fig. 6 are $\{(A_{111}, \overline{D_1M_1}, A_{12}, \overline{D_{12}M_{12}}), (A_{1121}, \overline{D_1M_1}, A_{12}, \overline{D_{12}M_{12}}), (A_{1122}, \overline{D_1M_1}, A_{12}, \overline{D_{12}M_{12}}), (A_{1123}, \overline{D_1M_1}, A_{12}, \overline{D_{12}M_{12}}), (A_2, \overline{D_2M_2})\}$. Each of these five mincuts represent a combination of certain events which will result in a successful attack if each of the corresponding event occurs. For example, an attack will be successfully launched if both attack events A_{1121} and A_{12} occur and both countermeasure events $\overline{D_1M_1}$ and $\overline{D_{12}M_{12}}$ fail at the same time in the mincut $(A_{1121}, \overline{D_1M_1}, A_{12}, \overline{D_{12}M_{12}})$.

D. PROBABILITY ANALYSIS IN ACT

In the attack countermeasure scenarios above, we obtain the mincut sets as one of the feasible solutions. However, it is important to determine the most critical event in ACT. Based on the discussed case, we present the event probability analysis of a successful attack to a single incident as follows.

We denote the probability of a successful false LSA attack in ACT as P_a, the probability of detecting attack type i as P_{D_i}, the probability of mitigating attack type i as P_{M_i}, the probability of a undetected false LSA attack in ACT as P_{ud}, and the probability of a detected but unmitigated false LSA attack in ACT as P_{um}. In this case (with countermeasures connected through an "AND" gate), the general function of a successful attack to a single component is

$$P_a = P_A \prod_{i=1}^{n} (1 - P_{D_i} \times P_{M_i}). \quad (13)$$

Fig. 7 shows P_a in a combination with and without countermeasures. From Fig. 7 we can see that P_a value for false LSA attack decreases with the incorporation of detection

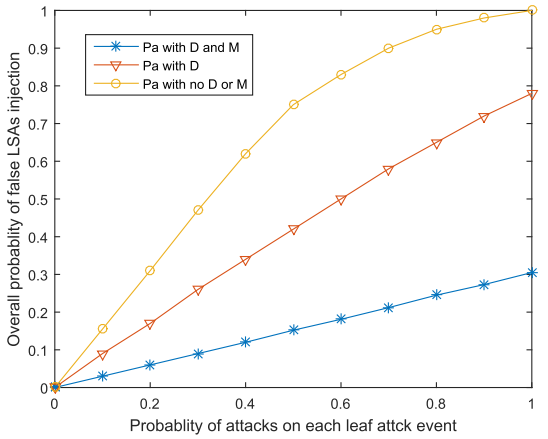


FIGURE 7. Comparison on P_a and probability values of attack of all the leaf nodes.

mechanisms, i.e. $P_a = P_{ud}$. With only detection mechanisms in ACT, mitigation are assumed to be perfect, i.e. they work with probability one. Therefore with the incorporation of mitigations (imperfect mitigation) in the ACT of false LSA attack, P_a increases ($P_a = P_{ud} + P_{um}$).

The probability (P_a) of an attack on false LSA injection is shown in Fig. 8, from the perspective of whether an effect of a single countermeasure DM_i would work for all the countermeasures. In this ACT example, the probability of a successful false LSA injection attack P_a would decrease rapidly as countermeasure strategies being taken effect.

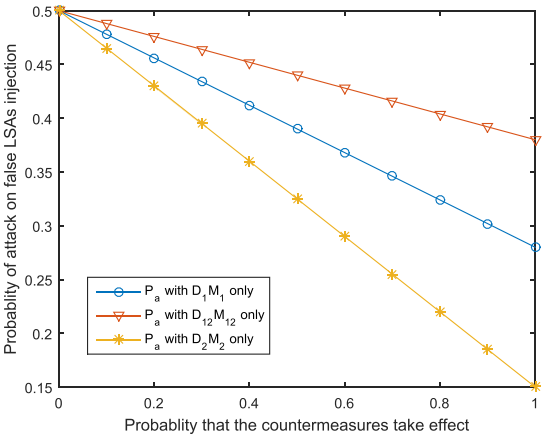


FIGURE 8. P_a against the probability that a countermeasure succeeds for LSA attack.

E. COST & IMPACT ANALYSIS

Cost can be grouped into two types: cost of attack C_A and security investment cost C_{SI}. In this case study, cost of an attack for an individual incident can be denoted as $\sum_{i=1}^{n} C_{A_i}$, and the corresponding impact on that is represented as $\sum_{i=1}^{n} I_{A_i}$. We select the minimum cost mincuts while computing C_A for this case, based on the assumption that an attacker would launch an attack at its minimum cost.

Security investment cost for ACT is computed by summing the security investment cost of countermeasures presented in the ACT.

As for impact analysis, even though countermeasures do not affect the impact value directly, countermeasures will result in reducing the risk which is the real expected value of impact [46]. In terms of risk to a system, it refers to the system's risk to a particular attack scenario. In this case study, two measures need to be taken into consideration. One is the impact, i.e., amount of damage that an attack scenario can affect the system I_a and the other one is the probability of attack success P_a. Combining the two, the risk to the system can be defined as the expected value of the impact. The expression for the system risk R for ACTs is

$$\mathrm{R} = P_a \times I_a. \tag{14}$$

Fig. 9 shows R of LSA ACT against probability of attack values (ranging uniformly from 0 to 0.5) and impact values of the NAN (ranging uniformly from $0 - 1 \times 10^3$).

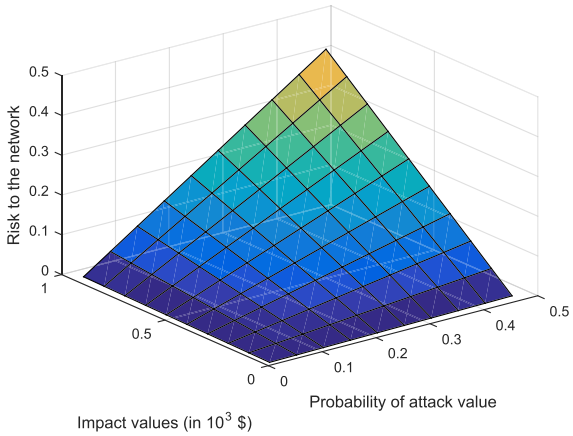


FIGURE 9. $Risk_{system}$ in the LSA attack scenario.

In this case study, we could also find out the changes brought by the deployment of necessary countermeasures significantly. The general function for the decrease in risk (ΔR_{DM_i}) for countermeasure (detection and mitigation schemes) DM_i can be given by

$$\begin{aligned}\Delta R &= \mathrm{R}_{\mathrm{no}DM_i} - \mathrm{R}_{\mathrm{with}DM_i} \\ &= (\mathrm{Pa}_{\mathrm{no}DM_i} - \mathrm{Pa}_{\mathrm{with}DM_i}) \times I_a.\end{aligned} \tag{15}$$

F. A SELF-HEALING NAN

According to the smart grid architecture depicted in Figs. 1 and 2, a NAN may consist of multiple mesh subnetworks, each of which is managed independently by its local gateway, i.e., DAP. However, due to the varying nature of the traffic, some gateways may suffer from more congestion than others. Under such conditions, nodes belonging to the same neighboring subnetwork cannot help each other in reducing the traffic load. In order to allow participation in the routing scheme, it would be a great advantage to combine all the subnetworks into a larger network with multiple gateways, i.e., DAPs, where all the meters can access to any of them.

Additionally, as we discussed earlier in Section IV, such a plan should enhance the self-healing and self-configuration abilities of the neighborhood area network if any gateway or node becomes inoperative.

1) RELIABILITY FACTORS

The first step towards achieving this is to develop flexible multi-gate routing scheme in such a way that meters can have an option to choose the best path to one of the DAPs. With such a routing flexibility together and with the help of an efficient packet scheduling technique, it would be possible to enhance network performance. Given the assumption in [25], we evaluate the networking failure to a DAP in Table. 1.

By reviewing the potential impacts and metrics, the loss of a DAP node and communication link between a concentrator and a DAP of NAN will increase the traffic in the local NAN and its neighbor NAN. Therefore, the increased network overhead may jeopardize the reliability requirements.

TABLE 1. Effects of networking failure to a DAP.

Failure Scenario	Potential Impact	Metrics
Failure on DAP node	Partial/full loss in DAP's subnetworks. Increase traffic in subnetwork adjacent to failed subnetwork	Failing rate, Connection Termination Probability
Failure on DAP-Concentrator link	Partial/full loss in subnetwork. Increase traffic in subnetwork adjacent to failed subnetwork	Failing rate, Link setup/release latency

We developed a simulation for self-healing neighborhood area network consisting of wireless mesh subnetworks, according to the scenario shown in Fig. 10. In this scenario each subnetwork is handled independently by its local DAP before being connected to the data concentrator. In this network, each node will hold a separate path to each of the gateways. The routing protocol for IEEE 802.11s, i.e., hybrid wireless mesh protocol [27], has been adopted as the core routing protocol in this simulation.

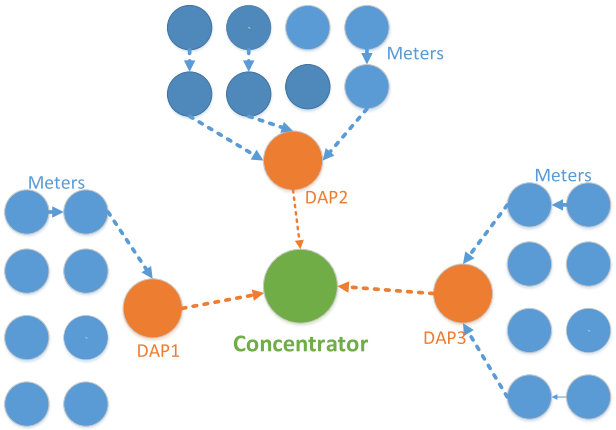


FIGURE 10. Multigate routing scheme for a self-healing NAN.

2) PERFORMANCE EVALUATION

We simulate different situations of failure cases, including one DAP failure as event A, link failure between a DAP and a concentrator as event B, and the combination of them along with one single DAP failure as event C.

In this scenario, as shown in Fig. 10, the network consists of mesh subnetworks, where nodes in each are handled by their local DAP. In this case, there are 8 meters (nodes) in each subnetwork and meters (nodes) are uniformly distributed within their coverage area. The simulation results are shown in Table 2.

TABLE 2. A simulation study on DAP failure.

Failure Scenario	Failing Rate (%)	Update Information Latency (s)
Event A	1.44	0.26
Event B	3.74	0.32
Event C	7.58	0.93

In the simulation environment for an overall throughput evaluation of the 3-DAP network, all nodes in the network generate data packets at variable bit rate (VBR) and the data is encapsulated into fixed 512 bits user datagram protocol (UDP) packets. In the PHY, IEEE 802.11b is used and the data-rate is 2 Mbps, while gateways are assumed to have an unlimited bandwidth. The noise factor set to 10, as recommended by IEEE 802.11b. The path loss factor set to 2 and the retransmission limit is 7. Based on the environment, we evaluate the network performance of the 3-DAP network in terms of overall throughput versus the input bit-rate per second per node. Table. 3 shows the results of the 3-DAP network according our simulation environment.

TABLE 3. A performance evaluation of 3-DAP network.

Input Bit Rate (kbps/node)	Throughput (%)
0.5	69.52
1.0	60.02
1.5	54.91
2.0	48.42
2.5	44.53
3.0	38.06
3.5	34.17
4.0	29.67
4.5	26.84

It is important to point out that due to the nature of the network, the routing announcement plays an important role in meeting the self-organization and self-healing requirements of the NAN. For instance, in the case of a smart meter malfunction, the root announcement can update the routing tree by trying to bypass the abnormal nodes.

As soon as a link breakage notification is received for this path, the source node will send the packet through the second route, while it updates its tree table to the first root (DAP). It should be noted that in both methods on-demand routing is used when a node experiences a link failure.

VIII. CONCLUSION

In this paper, we investigate the reliability issues of a NAN in smart grid. We start with the introduction of smart grid communication architecture, with a focus on the neighborhood area network, advanced metering infrastructure and the standard technologies deployed on them. We then present the reliability study. Specifically, we focus on reviewing reliability requirements and challenges of both communication components and network systems in NAN. By considering applications in smart grid NAN, reliable countermeasures strategies are demonstrated for coping with system crisis. We provide a comprehensive quantitative analysis for NAN in smart grid, using fault tree analysis on potential system failures and attack countermeasure tree to identify specific detection and mitigation strategies on malicious cyber attacks to communication systems in NAN. In addition, we conduct a simulation study that the self-healing ability of NAN is enhanced through proper topology design. The simulation study evaluates both reliability and networking performance of the communication networks in NAN, and the results have shown multi-gate routing could enhance the reliability of the network.

In our future work, we will continue the study for achieving high reliability of NAN, from the perspectives of both communication components and network systems, develop comprehensive and practical countermeasure strategies to potential reliability challenges, and design optimal schemes to achieve high availability to critical system components.

REFERENCES

[1] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, Feb. 2013.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, Oct. 2012.

[3] F. Ye, Y. Qian, and R. Q. Hu, "Energy efficient self-sustaining wireless neighborhood area network design for smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 220–229, Jan. 2015.

[4] F. Ye, Y. Qian, R. Q. Hu, and S. K. Das, "Reliable energy-efficient uplink transmission for neighborhood area networks in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2179–2188, Sep. 2015.

[5] F. Ye, Y. Qian, and R. Q. Hu, "Self-sustaining wireless neighborhood area network design for smart grid," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 2715–2720.

[6] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proc. Innov. Smart Grid Technol. Conf. Eur. (ISGT)*, Jan. 2010, pp. 1–7.

[7] S. H. Conrad, R. J. LeClaire, G. P. O'Reilly, and H. Uzunalioglu, "Critical national infrastructure reliability modeling and analysis," *Bell Labs Tech. J.*, vol. 11, no. 3, pp. 57–71, Apr. 2006.

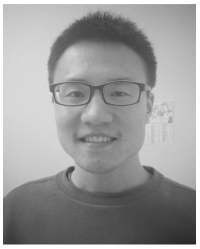
[8] K. S. Trivedi, D. S. Kim, A. Roy, and D. Medhi, "Dependability and security models," in *Proc. 7th Int. Workshop Design Rel. Commun. Netw. (DRCN)*, Oct. 2009, pp. 11–20.

[9] DOE, U.S., "Communications requirements of Smart Grid technologies," U.S. Dept. Energy, Washington, DC, USA, Tech. Rep., 2010, pp. 1–69.

[10] G. Yan, S. Eidenbenz, S. Thulasidasan, P. Datta, and V. Ramaswamy, "Criticality analysis of Internet infrastructure," *Comput. Netw.*, vol. 54, no. 7, pp. 1169–1182, 2010.

[11] D. Niyato, Q. Dong, P. Wang, and E. Hossain, "Optimizations of power consumption and supply in the smart grid: Analysis of the impact of data communication reliability," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 21–35, Mar. 2013.

[12] V. Kounev, M. Levesque, D. Tipper, and T. Gomes, "On smart grid communications reliability," in *Proc. 11th Int. Conf. Design Rel. Commun. Netw. (DRCN)*, Mar. 2015, pp. 33–40.
[13] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.
[14] S. Xu and Y. Qian, "Quantitative study of reliable communication infrastructure in smart grid NAN," in *Proc. 11th Int. Conf. Design Rel. Commun. Netw. (DRCN)*, Mar. 2015, pp. 93–94.
[15] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.
[16] NIST, U.S., *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*. Gaithersburg, MD, USA: Nat. Inst. Standards Technol., Sep. 2014, pp. 1–239.
[17] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: A survey," *IEEE Netw.*, vol. 28, no. 1, pp. 24–32, Jan./Feb. 2014.
[18] M. Erol-Kantarci and H. T. Mouftah, "Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 179–197, Mar. 2015.
[19] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.
[20] V. C. Gungor *et al.*, "Smart grid and smart homes: Key players and pilot projects," *IEEE Ind. Electron. Mag.*, vol. 6, no. 4, pp. 18–34, Dec. 2012.
[21] S. Paudyal, C. A. Canizares, and K. Bhattacharya, "Optimal operation of distribution feeders in smart grids," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4495–4503, Oct. 2011.
[22] T. Sauter and M. Lobashov, "End-to-end communication architecture for smart grids," *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1218–1228, Apr. 2011.
[23] A. Zaballos, A. Vallejo, and J. M. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Netw.*, vol. 25, no. 5, pp. 30–37, Sep./Oct. 2011.
[24] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–1, Sep. 2015.
[25] H. Gharavi and B. Hu, "Multigate communication network for smart grid," *Proc. IEEE*, vol. 99, no. 6, pp. 1028–1045, Jun. 2011.
[26] J.-S. Jung, K.-W. Lim, J.-B. Kim, Y.-B. Ko, Y. Kim, and S.-Y. Lee, "Improving IEEE 802.11s wireless mesh networks for reliable routing in the smart grid infrastructure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2011, pp. 1–5.
[27] *IEEE Draft Amendment to Standard for Information Technology Telecommunication and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking*, IEEE Standard P802.11s/D1.0, Nov. 2006.
[28] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks*, IEEE Standard 802.15.4g, Apr. 2012.
[29] *IEEE Draft Standard for Local and Metropolitan Area Networks Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment: Physical Layer (PHY) Specifications for Low Data Rate Wireless Smart Metering Utility Networks*, IEEE Standard P802.15.4g/D5, Aug. 2011.
[30] D. R. Shier, *Network Reliability and Algebraic Structures*. Oxford, U.K.: Clarendon, 1991.
[31] A. Yarali, "Wireless mesh networking technology for commercial and industrial customers," in *Proc. Can. Conf. Elect. Comput. Eng. (CCECE)*, May 2008, pp. 47–52.
[32] Q. Dong, D. Niyato, and P. Wang, "Dynamic spectrum access for meter data transmission in smart grid: Analysis of packet loss," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2012, pp. 1817–1822.
[33] D. Niyato, P. Wang, Z. Han, and E. Hossain, "Impact of packet loss on power demand estimation and power supply cost in smart grid," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2011, pp. 2024–2029.
[34] V. C. Gungor, D. Sahin, T. Kocak, and S. Ergüt, "Smart grid communications and networking," Türk Telekom, Altındağ, Turkey, Tech. Rep. 11316-01, Apr. 2011.
[35] F. Ye, Y. Qian, and R. Q. Hu, "A security protocol for advanced metering infrastructure in smart grid," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 649–654.
[36] J. Campbell, "Application of graph theoretic analysis to interindustry relationships: The example of Washington state," *Regional Sci. Urban Econ.*, vol. 5, no. 1, pp. 91–106, 1975.
[37] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440–442, Jun. 1998.
[38] *The Economic Cost of the Blackout: An Issue Paper on the Northeastern Blackout*, ICF Consulting, Fairfax, VA, USA, Aug. 2003.
[39] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.
[40] G. O'Reilly, A. Jrad, R. Nagarajan, T. Brown, and S. Conrad, "Critical infrastructure analysis of telecom for natural disasters," in *Proc. 12th Int. Telecommun. Netw. Strategy Planning Symp.*, Nov. 2006, pp. 1–6.
[41] G. O'Reilly, H. Uzunalioglu, S. Conrad, and W. Beyeler, "Inter-infrastructure simulations across telecom, power, and emergency services," in *Proc. 5th Int. Workshop Design Rel. Commun. Netw.*, Oct. 2005, pp. 16–19.
[42] P. Y. Kong, "Wireless neighborhood area networks with QoS support for demand response in smart grid," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–1, May 2015.
[43] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI)—A practical quantitative model," *J. Res. Pract. Inf. Technol.*, vol. 38, no. 1, pp. 55–66, 2006.
[44] R. T. Anderson, "Reliability design handbook," Rel. Anal. Center, Griffiss Air Force Base, NY, USA, Tech. Rep. RAC-RDH-376, 1976.
[45] A. Roy, D. S. Kim, and K. S. Trivedi, "Attack countermeasure trees (ACT): Towards unifying the constructs of attack and defense trees," *Secur. Commun. Netw.*, vol. 5, no. 8, pp. 929–943, 2012.
[46] T. Olzak. (Mar. 2006). *A Practical Approach to Threat Modeling*. [Online]. Available: http://adventuresinsecurity.com/blog/wp-content/uploads/2006/03/A_Practical_Approach_to_Threat_Modeling.pdf



SHENGJIE XU (S'14) received the M.S. degree in telecommunications from the University of Pittsburgh, PA, USA, in 2014. He is currently pursuing the Ph.D. degree with the Communication Networks and Security Laboratory, Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, USA. His research interests include smart grid communication networks, information assurance, and security in big data analytics.

YI QIAN (M'95–SM'07) received the Ph.D. degree in electrical engineering from Clemson University, Clemson, SC, USA. He was with the telecommunications industry, academia, and the government. Some of his previous professional positions include serving as a Senior Member of the Scientific Staff and Technical Advisor with Nortel Networks, a Senior Systems Engineer and Technical Advisor with several start-up companies, an Assistant Professor with the University of Puerto Rico at Mayagüez, and a Senior Researcher with the National Institute of Standards and Technology. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Nebraska–Lincoln. His research interests include network design, network modeling, simulation and performance analysis for next-generation wireless communication networks, wireless ad-hoc and sensor networks, vehicular networks, smart grid communication networks, high-speed networks and the Internet, and information assurance and network security. He is a member of ACM.

IEEE Access
The journal for rapid open access publishing

ROSE QINGYANG HU (S'95–M'98–SM'06) received the B.S. degree from the University of Science and Technology of China, the M.S. degree from the Polytechnic Institute of New York University, and the Ph.D. degree from the University of Kansas. She has over ten years of research and development experience with Nortel, Blackberry, and Intel as a Technical Manager, Senior Wireless System Architect, and Senior Research Scientist, actively participating in industrial 3G/4G technology development, standardization, system level simulation, and performance evaluation. She is currently an Associate Professor with the Electrical and Computer Engineering Department, Utah State University. She has authored extensively and holds numerous patents in her research areas. Her current research interests include next-generation wireless communications, wireless system design and optimization, green radios, multimedia quality of service (QoS)/quality of experience (QoE), communication and information security, wireless system modeling, and performance analysis. She is a member of the Phi Kappa Phi Honor Society and the Epsilon Pi Epsilon Honor Society. She was a recipient of best paper awards from the IEEE Globecom 2012 and IEEE ICC 2015. She is an IEEE Communications Society Distinguished Lecturer Class 2015–2016. She serves on the Editorial Boards of the *IEEE Wireless Communications Magazine*, the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, the IEEE INTERNET OF THINGS JOURNAL, the *Security and Communication Networks Journal*, *Wireless Communications and Mobile Computing*, and *KSII Transactions on Internet and Information Systems*. She has been a seven-time Guest Editor of the *IEEE Communications Magazine*, the *IEEE Wireless Communications Magazine*, and the *IEEE Network Magazine*. She served as the TPC Co-Chair of ICNC 2014, the TPC Vice Chair of the IEEE Greencom 2013, and the Symposium Co-Chair of the IEEE ICC 2012/2014/2015, the IEEE WCNC 2013, ICNC 2013, and the IEEE SmartgridComm 2012.